UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,859	02/27/2002	Melissa W. Dunn	MS# 180490.1 (MSFT 4969)	8746

321 7590 04/14/2005

SENNIGER POWERS LEAVITT AND ROEDEL
ONE METROPOLITAN SQUARE
16TH FLOOR
ST LOUIS, MO 63102

EXAMINER	
JOO, JOSHUA	

ART UNIT	PAPER NUMBER
2154	

DATE MAILED: 04/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/084,859	DUNN, MELISSA W.	
	Examiner	Art Unit	
	Joshua Joo	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/27/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. Claims 1-46 are presented for examination.

2. Claims 1-46 are rejected.

Claim Objections

3. Claims 24 and 43 are objected to because of the following informalities:

i) As per claim 24, "comprising" is followed by ";". It should be ":"

ii) As per claim 43, claim 43 starts on page 14, but it should start on the same page as claim 42, along with the claims following claim 43.

Claim Rejections - 35 USC § 112

4. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 24, the claim is dependent on itself. For this office action, claim 24 will be considered as depending on independent claim 22.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 22, 24, 26, 28, 40-41 are rejected under 35 U.S.C. 102(e) as being unpatentable by Desai et al, US Patent #6,820,204 (Desai hereinafter).

7. As per claim 22, Desai teaches an invention for selectively granting clients access to user's stored profile information. Desai's invention comprises of:

identifying the user (Col 9, lines 19-28; Col 14, lines 63-65. Client requests access to user's stored profile information, e.g. vendor and telemarketer.);

identifying a client of the web-services provider to which the user desires to grant access to the user-specific information in the data store (Col 8, lines 31-33; Col 9, lines 1-5; Col 14, lines 63-65. Client requests access to view user's stored profile information in an Internet network.);

identifying a method of access by which the user is willing to allow the client to access the user-specific information in the data store (Col 9, lines 9-14. User allows the client to view information on an element-by-element bases.);

identifying a level of access to the user-specific information in the data store the user desires to impose on the client (Col 9, lines 10-18. The user selectively grants access to the store profile information.); and

writing an access control rule to an access control list associated with said data store, said access control rule limiting access to the user-specific information in the data store by the client to the identified method and the identified level (Col 9, lines 19-22; Col 13, lines 25-33. User writes an access control rule that limits access to the user profile information by the identified method and level.).

8. As per claim 40, Desai teaches an invention for selectively granting clients access to user's stored profile information. Desai's invention comprises of:

obtaining at the web-services provider a digital request message from the third party desiring access to the user-specific information in the data store (Col 8, lines 31-34; Col 9, lines 1-4; Col 14, lines 61-64. Client requests access to user's stored profile information, where the user's stored profile information is stored on a web server.);

determining an intended purpose of third party accessing the user-specific information in the data store (Col 9, lines 19-31. Telemarketer, e.g. telemarketing.);

generating an option list having at least one entry therein based on the determined intended purpose of the third party for accessing the user-specific information in the data store (Col 9, lines 19-28; Col 13, lines 9-38. User generates a list based on purpose for the client to access user information. User allows vendor to view personal information while telemarketer is denied.);

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device (Col 8, lines 34-38, 63-65; Col 9, lines 27-31. User uses a computer running a web browser. User may selective grant access to each view to the clients. Telemarketer will be denied access to view user information.);

receiving from the network communication interface device a selection signal indicative of whether the user accepted or rejected the at least one option (Col 8, lines 63-65; Col 8, lines 27-31. User may selective grant access to each view to the clients. Telemarketer will be denied access to view user information.); and

creating an access control rule based on the received selection signal, said access control rule defining an extent of access to the user-specific information in the data store granted to the third party (Col 13, lines 8-32. User allows client to view selected data elements.).

9. As per claim 24, Desai teaches the method of claim 22 further comprising: exposing a menu to the user on the display interface of the network communication device, said menu allowing the user to identify the client, the method of access, and the level of access; and transmitting the identified client, the method of access, and the level of access to the web-services provider in a digital message format (Col 8, lines 34-38; Col 9, lines 10-30; Col 14, lines 7-15. Registered user uses a computer on a communication network. User may selectively grant access on an element-by-element basis for each view to a plurality of clients. A vendor is granted view access to telephone number and address by providing an access code or password, while a telemarketer may not be granted view access.).

10. As per claim 26, Desai teaches the method of claim 22 wherein identifying the level of access further comprises grouping the user-specific information in the data store into a plurality of information types and identifying which of said plurality of information types the client may access (Col 9, lines 10-30. The user-specific information in the data store is grouped and identified as to which information the client may access. Vendor may access telephone number and credit card number, while business contact may just view the user's telephone number.).

11. As per claims 28 and 41, Desai teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 22 (Col 11, lines 27-46. Information exchange system has software to perform necessary functions.).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and Robertson, US Patent #6,269,369.

14. As per claim 23, Desai does not teach the method of claim 22 further comprising identifying a subscription status, said subscription status indicating whether the user intends the client to be notified if the user-specific information in the data store changes.

15. Robertson teaches an invention for a contact management system, where clients may be permitted access to user's stored profile information. The contact manager determines whether any of the user's contacts need to be notified of changes to the user's information (Col 6, lines 48-54; Col 8, lines 17-23, 57-61).

16. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Robertson because both inventions deal with providing selective access to user's profile information. The teachings of Robertson to selectively issue notification to the users in an access list ensure that the user's clients have the most up-to-date information and the selective notification provides greater control to users in keeping information private.

17. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Desai and in view of Kramer et al, US Patent #5,414,852 (Kramer hereinafter).

18. As per claim 25, Desai does not teach the method of claim 22 wherein identifying the method of access further comprises identifying whether the client is permitted to modify the user-specific information in the data store.

19. Kramer teaches a method of protecting data in a computer system, where the user permits the client to modify files in a data store (Col 4, lines 1-5, 52-55).

20. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because both inventions deal with providing security to files and selectively allowing access to the files. The teachings of Kramer for the user to permit the client to modify files in the data store gives the user greater control of the client's type of access.

21. As per claim 27, Desai does not teach the method of claim 22 further comprising: authenticating a digital identity of the user prior to writing the access control rule to the access control list associated with the data store of user-specific information; and writing the access control rule to said access control list if the digital identity of the user is authenticated.

22. Kramer teaches of providing an identifier to access information on a computer system. The data manager controls an access list, which contains the identifiers of the users, where the data manager may provide writing access of the user's authorized access. The data manager application is invoked when user desires to access to files (Col 3, lines 15-34; Col 4, lines 49-55).

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Desai and Kramer because both inventions deal with providing clients selective access to information stored on a computer network. The teachings of Kramer for a user to provide an identifier, and to modify the authorized user's access conditions would allow clients to modify user information as needed, and it would increase the security by preventing unauthorized users to different forms of access.

24. Claims 15-19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita and in view of Desai, US Publication #2002/0095571.

25. As per claim 15, Orita teaches an invention for providing security in accessing files over a computer network. Orita's invention comprises of:

operatively receiving at the host computer a request from the client to access information in the data store (Col 3, lines 10-13, 56-61. Host computer receives a request from the client to access specified files.);

determining an intended use by the client of the information in the data store (Col 4, lines 16-18, 60-63. Client provides data indicating the access type, where access type can be deleted, modifying, writing, and reading.);

determining an allowed level of access permitted by the user (Col 4, lines 34-36, 52-67. Host computer determines the authority level and the access type of user based on the access protection information.);

comparing the determined intended use with the determined allowed level of access (Col 4, lines 34-36, 52-67. Host computer determines the authority level and the access type of user based on the access protection information.), and

completing the request from the client to access information in the data store when the determined intended use is within the determined allowed level of access (Col 4, lines 64-68. Request is completed if the type of access is allowed.).

26. Orita does not specifically teach of receiving at a web-services provider a request from the client to access information that is user-specific.

27. Desai teaches an invention for information exchange, where a user allows selective access to clients of user's profile information. The user's profile information is stored on an information exchange server, accessible through the Internet (Col 8, lines 17-35; Col 9, lines 10-14).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both inventions deal with providing selective access to information stored on a database. The teachings of Desai for the information to be user-specific and located on a web server allow the user's profile information to be more accessible to other users. It also allows for a fast and convenient method for the exchange of information with clients, such as improving methods of transactions.

29. As per claim 16, Orita teaches the method of claim 15 wherein determining the intended use by the client of the user-specific information in the data store comprises: determining a type of information within the user-specific information in the data store that is being requested by the client; and determining a form of access to the user-specific information in the data store that is

being requested by the client (Col 3, lines 56-69; Col 4, lines 16-19. Client request information by specifying a file name and indicates type of access.).

30. As per claim 17, Orita teaches the method of claim 16 wherein comparing the determined intended use with the determined allowed level of access comprises: determining if the user permits access to the type of information within the user-specific information in the data store that is being requested by the client; and determining if the user permits the form of access to the user-specific information in the data store that is being requested by the client (Col 3, line2 – Col 4, lines 8; Col 4, lines 55-64. Host computer determines if the client is permitted access to the type of information being requested and determines if the form of access is permitted.).

31. As per claim 18, Orita teaches the method of claim 17 further comprising: creating an access filter, said access filter defining an extent to which the user permits access to the type of information within the user-specific information in the data store and an extent to which the user permits the form of access to the user-specific information in the data store (Col 3, lines 33-52. Host computer creates an authority level, indicating an extent to which the host computer permits access to the type of information and, an authority level-altering data.); and

wherein completing the request from the client to access the user-specific information in the data store when the determined intended use is within the determined allowed level of access further comprises (Col 3, line 1- Col 4, lines 8. The allowed level of access is determined by comparing the authority level needed and the requesting authority level.):

applying the access filter to the user-specific information in the data store to create a filtered information set; and permitting the client to access filtered information set (Col 3, lines 41-52. Files having a certain level are permitted access.).

32. As per claim 19, Orita teaches the method of claim 15 further comprising denying the client access to the requested user-specific information in the data store if the determined intended use is outside the allowed level of access (Col 3, line 1–Col 4, line 3; Col 4, lines 52-64. Client is denied if the authority level is outside the allowed level of access.).

33. As per claim 21, Orita teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 15 (Col 2, lines 58-60. Host computer performs the necessary process for the invention.).

34. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita and Desai, and in view of Kramer, US Patent #5,414,852.

35. As per claim 20, Orita does not teach the method of claim 15 further comprising invoking a consent engine if the determined intended use is outside the allowed level of access, said consent engine informing the user of the client's request to access the user-specific information in the data store and inviting the user to permit or deny the client's request to access the user-specific information in the data store.

36. Kramer teaches an invention for protecting data in a computer system, where a data manager can update the access control list to add or remove clients and to permit or deny the client's type of access (Col 4, lines 1-5, 52-55).

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Kramer because these inventions deal with providing security in accessing information. Orita teaches an invention where access is based on access protection information, where a client's access is based on meeting parameters of an access list. Thus, it would be desirable for Orita's invention to update the access list to allow read or write conditions because doing so would provide greater control to the user of who can access information, and it ensures that user access is appropriate.

38. Claims 1-3, 7, 8, 10, 14, 29, 30, 35-36, 39, 44-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, US Patent #5,163,147, and in view of Bradee et al, US Publication #2002/0095571 (Bradee hereinafter), and Desai, US Patent #6,820,204.

39. As per claims 1, 29, 38, 44, 45, 46, Orita teaches an invention for providing security in accessing files over a computer network. Orita's invention comprises of:

obtaining an access request message from the client and directed to the software service requesting user-specific information, said request message including an access request parameter indicating the client's requested form of access to the user-specific information in the data store (Col 4, lines 16-18, 23-24. Client sends request to access information e.g. specified files, indicating the type of access.);

comparing the access request parameter to an access control list associated with the software service, said access control list identifying whether the user has granted the form of access requested by the client (Col 4, lines 34-36, 52-55, 60-64. Determines if the client has permission based on access protection level.);

permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access requested by the client (Col 4, lines 66-67. Client is permitted access if the type of access is granted.); and

invoking an access control engine if the user has not previously granted the form of access requested by the client, said access control engine (Col 4, line 65-Col 5, line 1. Host computer determines if client is provided the form of access by either allowing or denying access.):

determining an intended use by the client of the requested user-specific information in the data store (Col 4, lines 16-18, 60-62. Client indicates type of access such as read or write.);

comparing the determined intended use by the client with a default access control instruction (Col 4, line 65-Col 5, line 1. Determines if client is provided the form of access by either allowing or denying access based on access protection information.);

transmitting a fault response to the client if the default access control instruction does not permit the determined intended use (Col 4, line 68- Col 5, line 1. Access is denied.).

40. Orita does not teach of dynamically updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use.

41. Bradee teaches of dynamically updating an access control list to permit the client to have access to information on a web server if the instructions permit the client for viewing of the information (Page 8, Paragraph 62).

42. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Bradee because both inventions deal with providing

security on a computer system. The teachings of Bradee to dynamically update the user access list allow clients to view information that wasn't accessible when the clients meet predefined parameters.

43. Orita does not specifically teach of a web-service provider maintaining a data store of information that is user-specific.

44. Desai teaches an invention for information exchange, where the user allows clients selective access to the user's profile information. The user's profile information is stored on an information exchange server, accessible by the Internet (Col 8, lines 17-35; Col 9, lines 10-14).

45. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both inventions deal with providing selective access to information stored on a database. The teachings of Desai for the information to be user-specific and located on a web server, allow for an efficient method for exchanging user information. By having the information on a web server, the information is more accessible to clients and allows for faster exchange of information with clients as well, such as improve methods for transactions.

46. As per claim 2, Orita teaches the method of claim wherein comparing the determined intended use by the client with the default access control instruction further comprises comparing the client's requested form of access to the default access control instruction to determine if the default access control instruction permits the requested form of access (Col 4, lines 52-67. Determines access by comparing the intended use by the client and the access conditions to which the client is allowed.).

47. As per claim 3, Orita teaches the method of claim 1 wherein the client's requested form of access to the user-specific information in the data store identifies a desired subject matter to be accessed and a method of accessing the desired subject matter and wherein comparing the determined intended use by the client with the default access control instruction further comprises: determining if the default access control instruction permits the client to access the desired subject matter; and determining if the default access control instruction permits the identified method of accessing the desired subject matter (Col 3, lines 10-13, 40-51; Col 4, lines 16-18, 55-67. Host computer determines if client is allowed access to the file, and determines if the access protection information allows the identified method of accessing the file e.g. deleting, modifying, writing, and reading.).

48. As per claims 7 and 35, Orita teaches the invention further comprising authenticating a digital identity of the user and denying access to the requested user-specific information in the data store if the digital identity of the user is not authenticated (Col 3, lines 10-14, 56-59. User provides ID information and password. Access is denied if the identity of the user is not authenticated.).

49. As per claims 8 and 36, Orita teaches the invention, wherein determining the intended use by the client of the requested user-specific information further comprises obtaining a copy of an intentions document associated with the client, said intentions document including a field being indicative of the intended use by the client of the requested user-specific information (Col 4, lines 16-18, 57-68. Client sends data indicating access type to the host computer. With the information host computer can determine if access is allowed.).

50. As per claim 10, Orita teaches the method of claim 1 wherein permitting the client to have access to the requested user-specific information in the data store if the user has granted the form of access request by the client further comprises: permitting the client to read the requested user-specific information in the data store; and permitting the client to write the requested user-specific information in the data store (Col 4, lines 16-18, 60-63. Type of access by the client may be reading and writing the information in the data store.).

51. As per claim 14, Desai teaches one or more computer-readable media having computer-executable instructions for performing the method recited in claim 1 (Col 11, lines 27-46. Information exchange system has software to perform necessary functions.).

52. As per claim 30, Orita does not teach of a system comprising a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device.

53. Desai teaches that the network device may be a computer running a web browser application and has a selection menu. The network device is adapted to communicate with the information exchange server (Col 8, lines 14-36; Col 13, lines 53-66).

54. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Desai because both inventions deal with providing selective access to information stored on a database. The teachings of Desai to have a display interface and selection menu, on a network device that is connected to the web server would

allow the user to select which clients are granted access to user information stored on the web server.

55. As per claim 39, Orita teaches the system of claim 38 wherein the access control interface comprises a service-side fabric associated with the software service provided by the web-services system (Col 4, lines 53-68. Host computer controls access to information stored on database.).

56. Claims 4, 5, 13, 31-34, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Bradee, and Desai, and in view of Kramer, US Patent #5,414,852.

57. As per claims 4, 5, 31-34 Orita does not teach the method, wherein the user communicates with the web-services provider via network communication device having a display interface and a selection interface, the method further comprising:

generating an option list having at least one entry therein based on the determined intended use by the client of the requested user-specific information in the data store;

displaying to the user on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option using the selection interface of the network communication device;

receiving from the network communication device a selection signal indicative of whether the user accepted or rejected the at least one option; and

creating an access control rule based on the received selection signal, said access control rule defining the extent of access to the requested user-specific information in the data store granted to the client.

creating the access control rule comprises updating the access control list such that the access control reflects whether the user accepted or rejected the at least one option.

58. Kramer teaches an invention for protecting data in a computer system where an access list is created based on intended use by the data manager. The data manager has the option to modify the access list, adding or deleting users, and changing the access permissions for the users. The access list is used to define the extent of access to the requester of the information (Col 3, lines 64-Col 4, lines 1-6, 53-55).

59. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Kramer because both inventions deal with providing security in accessing information. Orita teaches an invention where access is based on access protection information, where a client's access is based on meeting parameters of an access list. Thus it would be desirable for Orita's invention to include the method of generating an access list to provide the conditions and having the option of changing the access permission because doing so would provide to the user more control of who can access information.

60. As per claim 13, Orita does not teach the method of claim 1 wherein updating the access control list to permit the client to have access to the requested user-specific information in the data store if the default access control instruction permits the determined intended use further comprises: updating the access control list to permit the client to read the requested user-specific information in the data store; and updating the access control list to permit the client to write the requested user-specific information in the data store.

61. Kramer teaches the invention where the access list is updated to permit the client to read and write the requested data file (Col 4, lines 49-55).

62. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Kramer because these inventions deal with providing security to access files, where each individual file has different access parameters. Orita teaches an invention where access is based on access protection information, where a client's access is based on meeting parameters of an access list. Thus it would be desirable for Orita's invention to update the access list to provide the conditions and having the option of changing the access permission such as allowing read and write access because doing so would provide greater control to the user of who can access information.

63. As per claim 37, Orita does not teach the system of claim 36 further comprising: a network communication device having a display interface and a selection menu and wherein the user communicates with the web-services provider via the network communication device; and a consent engine retrieving the client intentions document and generating an option list having at least one entry therein based on the intended use identified in the intentions document, said consent engine displaying on the display interface of the network communication device an option menu reflecting the generated option list, said option menu prompting the user to accept or reject at least one option displayed on the option menu using the selection interface of the network communication device.

64. Kramer teaches an invention for protecting data in a computer system where an access list is created based on intended use by the data manager. The data manager has the option to modify the access list, adding or deleting users, and changing the access permissions for the

users. The access list is used to define the extent of access to the requester of the information (Col 3, lines 64-Col 4, lines 1-6, 53-55).

65. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Kramer because both inventions deal with providing security in accessing information. Orita teaches an invention where access is based on access protection information, where a client's access is based on meeting parameters of an access list. Thus it would be desirable for Orita's invention to include the method of generating an access list to provide the conditions and having the option of changing the access permission because doing so would provide to the user more control of who can access information.

66. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Bradee, and Desai, and in view of Allgeier, US Patent #5,995,972.

67. As per claim 6, Orita does not teach the method of claim 1 further comprising: determining if the client has a local copy of the requested user-specific information in the data store before transmitting the access request message; and retrieving said local copy of the requested user-specific information if the local is available; determining if said local copy of the requested user-specific information is current; and transmitting the access request message only if said local copy of the requested user-specific information is not available and not current.

68. Allgeier teaches an invention where a determination is made if a selected data is stored in a first database. If the selected data is available, it is retrieved. The invention checks to see if the selected data in the first database is current. If the selected data is not current or not available, the second database is queried and accessed for the selected data.

69. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Allgeier because both inventions deal with accessing information over a computer network. The teachings of Allgeier to determine if local data is available and to request access to data at secondary location if the data is not available or not current improves the invention of Orita because data is transferred from the computer to the client on an needed basis. This would improve network efficiency since this prevents large amounts of data from being transferred on fixed bases.

70. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Bradee, and Desai, and in view of Robertson, US Patent #6,269,369.

71. As per claim 9, Orita does not teach method of claim 1 further comprising: determining if the client has an access subscription right to the requested user-specific information in the data store; and permitting the client to have access to the requested user-specific information in the data store if the client has access subscription right to the requested user-specific information in the data store.

72 Robertson teaches an invention for managing which clients may have access to user information. The contact manager provides notification of changes to the user's information to the list of clients. The clients are allowed access to the user information (Col 6, lines 48-54; Col 8, lines 17-23, 57-61).

73. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Robertson because both inventions deal with being granted access to information. The teachings of Robertson to issue a notification to the users in

an access list and allowing access to that information allows the host computer to specify permission separately for each user, depending on his access permission.

74. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, Bradee, and Desai, and in view of Erickson et al, US Publication #2003/0081791 (Erickson hereinafter).

75. As per claim 11, Orita teaches the method wherein permitting the client to read the requested user-specific information in the data store comprises accessing said requested user-specific information and transmitting a copy of the access requested user-specific information to the client (Col 4, lines 66-68; Col 5, lines 8-12. Client is allowed access to read the requested information on the host computer, where the contents of the information are displayed on screen.).

76. Orita does not teach that the information is send in a SOAP message.

77. Erickson teaches an invention for transmitting messages according to the SOAP protocol (Page 2, Paragraph 21).

78. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Erickson because both inventions deal with providing increased security with accessing files. The teachings of Erikson to use the SOAP protocol in sending messages would improve Orita's invention because it would provide increased security because the messages contain a public key in the header and a session key for the data, thus providing encryption.

79. As per claim 12, Orita teaches the method wherein permitting the client to write the requested user-specific information in the data store comprises receiving at the host computer a message from the client identifying the requested user-specific information and writing the identified requested user-specific information in the data store (Col 3, lines 57-60; Col 4, lines 61-68; Col 5, lines 8-13. Client is permitted to write the information in the host computer, where the host computer receives a request for the information and writing the identified information.).

80. Orita does not teach of receiving at the web-services provider a SOAP message from the client.

81. Erickson teaches an invention for transmitting messages according to the SOAP protocol (Page 2, Paragraph 21).

82. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Erickson because both inventions deal with providing increased security with accessing files. The teachings of Erikson to use the SOAP protocol in sending messages would improve Orita's invention because it would provide increased security because the messages would contain a public key in the header and a session key for the data, thus providing encryption.

83. Claims 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orita, #5,163,147, and in view of Bradee, US Publication #2002/0095571,and Kramer, US Patent #5,414,852.

84. As per claim 44, Orita teaches an invention for providing security in accessing files over a computer network. Orita's invention comprises of:

retrieving an intentions document associated with the third party desiring access to the user-specific information in the data store, said intentions document identifying (Col 3, lines 10-14; Col 3, lines 56-61. Clients sends request to access data.):

a purpose for which the third party desires access to the user-specific information in the data store (Col 3, lines 56-61; Col 4, lines 16-19. Client indicates the type of access.);

a method by which the third party proposes to access the user-specific information in the data store (Col 3, lines 56-61; Col 4, lines 16-19. Client indicates the type of access.);

an identity of the third party (Col 3, lines 10-13, lines 56-61. User provides ID and password.);

the user-specific information in the data store to which the third party desires access (Col 3, lines 10-13, lines 56-61. User indicates data user desires to access.);

the purpose for which the third party desires access to the user-specific information in the data store (Col 3, lines 56-61; Col 4, lines 16-19. Client indicates the type of access.);

the method by which the third party proposes to access the users-specific information in the data store (Col 3, lines 56-61; Col 4, lines 16-19. Client indicates the type of access.);

prompting the user to authorize or deny the third party to access the user-specific information in the data store (Col 4, lines 51-68. Host computer authorizes or denies the user access to the user information.); and

operatively receiving a selection signal being indicative of whether the user authorized or denied the third party to access the user-specific information in the data store.

85. Orita does not teach the value proposition associated with the purpose for which the third party desires access to the user-specific information in the data store and creating an

access control rule indicative of whether the user authorized the third party to access the user-specific information in the data store.

86. Bradee teaches an invention for selectively allowing access to information stored on a web server where the client pays to view the information. Bradee also teaches of dynamically updating the access list to allow the client access to the stored information (Page 8, Paragraph 0062)

87. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Bradee because both inventions deal with providing security on a computer system. The teachings of Bradee for the user to offer a value proposition and to dynamically update the user access list allow the client to view certain information on the web server when the client meets certain conditions set forth by the user.

88. Orita does not teach of displaying the menu entities on the menu on the display interface of the network communication device;

89. Kramer teaches of protecting data in a computer system where the data manager may modify the access list, allowing the data manager to allow or deny access to the information (Col 14, lines 49-55).

90. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Orita and Kramer because both inventions deal with providing security in accessing information. Orita teaches an invention where access is based on access protection information, where a client's access is based on meeting parameters of an

access list. Thus it would be desirable for Orita's invention to have a display menu because it would allow the user to change the access permission.

91. As per claim 43, Orita teaches the system of claim 42 wherein the access control interface comprises a service-side fabric associated with the software service provided by the web-services system (Col 4, lines 53-68. Host computer controls access to information stored on database.).

Conclusion

92. A shortened statutory period for reply to this Office action is set to expire THREE MONTHS from the mailing date of this action.

93. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joshua Joo whose telephone number is 571 272-3966 and fax number is 571 273-3966. The examiner can normally be reached on Monday to Thursday 8 to 5:30.

94. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on 571 272-3964.

95. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

April 3, 2005
JJ

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100